CLAIMS

1. A method of access to a service with fast authentication and revocable anonymity, characterized in that it comprises the steps of:

i) identifying and registering a client (C) and providing him with means for authenticating himself to an anonymous certification authority (ACA),

ii) authenticating the client to the anonymous certification authority using the means provided in step i) and supplying means enabling him to authenticate himself anonymously to a server (Se),

iii) authenticating the client by producing an anonymous signature and opening and maintaining an anonymous authentication session with a server (Se), and

iv) selectively allowing contact between the server (Se) and the anonymous certification authority (ACA) to revoke the anonymity of the client (C) using the signature provided in step iii).

2. A method according to claim 1, characterized in that it comprises, before the step ii), an additional step of communication between the anonymous certification authority (ACA) and the server (Se) whereby the server (Se) presents to said authority (ACA) a request to obtain means enabling verification of the anonymous authentication supplied by a client (C).

3. A method according to claim 1 or claim 2, characterized in that the step iii) comprises three stages:

. a first stage in which the client (C) calculates data formed of a series of tokens of which one enables a session to be opened and the others enable that session to be maintained,

. a second stage in which the client (C) makes a strong undertaking to the server as to the series of tokens, and

. a third stage of maintaining the session with the aid of the series of tokens.

4. A method according to claim 3, characterized in that all the tokens are for one-time use and strongly interdependent.

5. A method according to either claim 3 or claim 4, characterized in that the token generation step uses two cryptographic primitives, namely a hashing function and a random number.

6. A method according to claim 5, characterized in that the first token is obtained by applying the hashing function to the random number, the second token is obtained by applying the hashing function to the first token obtained, and so on until n tokens are obtained:

$$H(W_0) = W_1;\ H(W_{n-1}) = W_n.$$

7. A method according to any one of claims 3 to 6, characterized in that the second stage includes obtaining an anonymous signature of an initialization token W_n enabling authentication of a client by the server.

8. A method according to any one of claims 3 to 7, characterized in that information such as a numerical value is associated with the initialization token.

9. A method according to any one of claims 3 to 8, characterized in that on each new authentication the client (C) sends the server (Se) a token of at least one unit lower rank than that previously used.

10. A method according to any one of claims 3 to 9, characterized in that on each new authentication the client (C) sends the server (Se) a token W_i whose rank (i) is selected to be representative of the value of an

operation, for example a number of bid increments.

11. A method according to any one of claims 1 to 10, characterized in that it is applied to bidding and the steps of the client (C) submitting an increased bid are effected by sending successive tokens of lower rank.

12. A method according to any one of claims 1 to 11, characterized in that it uses a group signature by associating a plurality of identifiers and respective private keys with a single group public key.

13. A method according to any one of claims 1 to 12, characterized in that it uses a blind signature.

14. A method according to either claim 12 or claim 13, characterized in that the powers to revoke anonymity are divided between two or more authorities.

15. A system adapted to open and maintain an authentication session guaranteeing non-repudiation, characterized in that it comprises means adapted to implement three stages:

. a first stage in which the client (C) calculates data formed of a series of tokens of which one enables a session to be opened and the others enable that session to be maintained,

. a second stage in which the client (C) makes a strong undertaking to the server as to the series of tokens, and

. a third stage of maintaining the session with the aid of the series of tokens.

16. A method according to claim 15, characterized in that the token generation step uses two cryptographic primitives, namely a hashing function and a random number.

17. A method according to either claim 15 or claim 16, characterized in that it uses a group signature by associating a plurality of identifiers and respective private keys with a single group public key.

18. A method according to any one of claims 15 to 17, characterized in that it uses a blind signature.

19. A method according to any one of claims 15 to 18, characterized in that the powers to revoke anonymity are divided between two or more authorities.